NASA Procedural Requirements

NPR 1600.3
Effective Date: May 31, 2012
Expiration Date: May 31, 2017

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Personnel Security (Change 2, April 29, 2013)

Responsible Office: Office of Protective Services

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | ALL |

Chapter 1. Introduction

1.1 Overview

1.1.1 The NASA Administrator is responsible for implementing a comprehensive and effective personnel security program for the Agency. Personnel Security Investigations (PSI) are used to:

a. Evaluate the character and conduct of Government workers for the purpose of making suitability determinations for covered positions and continuous evaluation through reinvestigations of individuals in positions of public trust as required by Executive Order (EO) 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Position of Trust, and 5 CFR pt. 731, Suitability.

b. Evaluate the character and conduct of contractor workers by making fitness determinations for contractor employment per contractual requirements.

c. Evaluate the character and conduct of Government workers for excepted service or other non-covered positions.

d. Determine the eligibility of Federal employees for national security positions under EO 10450, Security Requirements for Government Employment, the eligibility for a clearance to access classified information under EO 12968, Access to Classified Information; continuous evaluation through reinvestigation of individuals holding clearances; and 5 CFR pt. 732, National Security Positions.

e. Determine the eligibility under Federal Information Processing Standards, (FIPS 201), "Personnel Identity Verification (PIV) of Federal Employees and Contractors," March 2006, as amended, and Homeland Security Presidential Directive 12 (HSPD-12) for Personal Identity Verification (PIV) as mandated in Federal Information Processing Standards (FIPS) Publication 201-1 for access to Federal facilities and federally controlled information systems. Specifics for PIV processing are outlined in FIPS SP 800-79-1 and referenced in Draft NPR 1600.6, NASA Identity and Credential Management.

1.2 Responsibilities

1.2.1 Assistant Administrator, Office of Protective Services (AA, OPS). The AA, OPS shall:

a. Establish and maintain an efficient personnel security program in accordance with Federal standards consistent with current personnel security/fitness policies, procedural requirements, and guidelines as established by the Security Executive Agent, Director of National Intelligence, and the Suitability Executive Agent, Office of Personnel Management (OPM).

b. Establish and maintain the NASA Central Adjudication Facility (CAF). CAF personnel shall be responsible for adjudicating all PSI results to determine a civil service employee's eligibility for initial or continuing access to Classified National Security Information (CNSI).

c. Serve as Agency Advocate for Electronic Questionnaires for Investigation Processing (e-QIP) and be responsible for designing specific policy, program management, and execution of the e-QIP system.

1.2.2 Center Directors shall:

a. Ensure the Center Chief of Security/Center Chief of Protective Services (CCS/CCPS) manages the Center personnel security program in accordance with this NPR.

b. Ensure full Center compliance with the provisions set forth in this chapter.

1.2.3 The CCS/CCPS shall:

a. Designate a Federal civil service employee with a satisfactorily adjudicated PSI on file with OPM to serve in the role of Program Manager in e-QIP. This employee is responsible for administering e-QIP at the Center level and training new e-QIP users.

b. Process and submit all PSI requests to OPM electronically. E-QIP is mandated for use to submit PSIs for civil service and contractor employees to OPM.

c. Ensure that a check of OPM databases such as Personnel Investigations Processing System/Central Verification System (PIPS/CVS) is performed to identify any previous investigation that will serve reciprocally before initiating a PSI. The acceptance of prior determinations will be based on an equivalent investigation and evidence of a favorably adjudicated investigation on the individual.

d. Maintain close coordination with OPM Investigations Service (OPM-IS) and Federal Investigations Processing Service (OPM-FIPS) and process the appropriate requests for PSIs.

e. Ensure adjudications for credentialing are performed by senior personnel security specialists who have been trained in adjudication by an accredited provider.

f. Process security clearance requests for employees under their jurisdiction, subject to the eligibility standards set forth in this chapter.

g. Notify the NASA CAF of any adverse information regarding any civil service employee at the Center that holds a National Security clearance or assignment to a sensitive position.

h. Require NASA civil service employees granted a security clearance to execute a Classified Information Nondisclosure Statement (SF 312) in accordance with 32 C.F.R. 2003, National Security Information, prior to access to national security information. i. Suspend a civil service employee's clearance access "for cause" based on developed disqualifying adverse information under the Continuous Evaluation Program.

j. Perform an annual review of civil service employee clearance holders and access requirements to ensure Center personnel security clearance needs are properly managed. The CCS/CCPS will develop and implement the appropriate local procedures necessary to ensure the review is conducted.

k. In cooperation with Office of Human Capital Management (OHCM) Resource Specialists, determine the sensitivity designation for national security position for all existing and newly established civil service positions whose duties clearly reflect the requirement for access to CNSI.

l. Refer all employment suitability cases for NASA civil service employees to the appropriate OHCM for review and adjudication upon receipt of the OPM Report of Investigation (ROI).

m. Assist OHCM personnel by conducting local records checks or automated record checks such as the Central Verification System (CVS), to clarify, expand, or mitigate information that has been provided by the investigation provider or a Department of Justice, National Crime Information Center (NCIC) query when requested.

n. Maintain in accordance with the Privacy Act and existing NASA system of records, individual personnel security files on all investigated personnel. Review applicable reports with officials in the review process who shall make the determination relative to continued access or revocation of access privileges. Security files will contain:

(1) Copies in Center personnel security file of the OPM Case Closing Transmittal, Certification of Investigation, signed e-QIP release sheets, and a signed and dated copy of the OPM Form OF79A for civil service and contractor employees. NASA CAF personnel will maintain copies of the OPM Form OF79A for Federal employees processed for security clearances.

(2) Any adverse information reports on affected contractor or civil service employees.

(3) Copies of concurrence documentation from Office of International and Interagency Relations (OIIR) for any foreign national granted access to classified information.

(4) Signed copies of Classified Information Nondisclosure Agreements Standard Form 312 (SF 312) for NASA civil service employees who have access to Classified National Security Information (CNSI).

(5) Inform all investigated personnel their rights to request under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (3 U.S.C. 552a), as applicable, any documents, records, and reports upon which an investigation was conducted.

1.2.4 The CCS/CCPS shall establish written procedures for the following:

a. Maintaining personnel security electronic files and distribution instructions for the completion of all electronic forms for the investigation process.

b. Assuring the appropriate investigation has been conducted for each NASA Federal or contractor employee.

c. Referring medical related data in investigative files to the appropriate medical authority for review and evaluation if needed to make a credentialing decision.

d. Conducting local records checks or automated records checks when necessary to clarify, expand, or mitigate information that has been forwarded to the CCS/CCPS.

e. Making appropriate notifications for confirmation of the results of a favorable access determination or actions as a result of a non-favorable access determination.

1.2.5 The Center OHCM organizations shall:

a. Ensure that appropriate management and supervisory personnel identify and develop the position descriptions for positions that require access to CNSI. These position descriptions will reflect the level of national security access.

b. Ensure no recruitment, hiring, or change of position action takes place until the appropriate position sensitivity level and risk designation has been established and the position description has been updated to reflect the change.

c. Cooperate with security officials during security inquiries and investigations pertaining to the requirements of this chapter.

1.2.6 The Director, OHCM at each Center shall:

a. Designate all covered positions as high, moderate, or low risk as determined by the potential for adverse impact to the efficiency and integrity of the service.

b. Verify employment eligibility of a civil service new hire. Review OPM Form OF 306, Declaration for Federal Employment Form documents for new hires. Review I-9 documents or coordinate the review with CCS/CCPS.

c. Grant reciprocity to prior suitability determinations in accordance with 5 C.F.R. pt 731 or ensure e-QIP is transmitted to OPM on a civil service new hire no later than 14 days after entry on duty (EOD) date.

d. Ensure that supervisors are advised on the proper processing of any personnel who may be reassigned or are the subject of other personnel actions, including termination, resulting from the revocation of security clearance.

1.2.7 Managers and supervisors shall:

a. Ensure full compliance with the requirements established in this policy.

b. Jointly with OHCM, ensure appropriate and accurate position risk designation and sensitivity levels are assigned for all civil service employees under their purview.

c. Assist OHCM personnel during the suitability determination process.

d. Ensure that civil service employees requiring reinvestigation are initiated according to OPM and OHCM position risk and sensitivity levels requirements.

1.2.8 The NASA General Counsel or the Chief Counsel of each Center shall provide legal counsel with regard to implementation of this NPR.

1.2.9 Contract Management Officials (Contractor Management, Contracting Officer, Contracting Officer's Technical Representative (COTR), and Project Managers) shall:

a. Ensure full compliance with this NPR.

b. Coordinate with the CCS/CCPS for the designation of risk for contractor employees and the timely on boarding of contractor employees.

1.3 Waivers and Exceptions

1.3.1 Centers may occasionally experience difficulty in meeting specific security requirements established by NASA policy. The process for submitting requests for waivers or exceptions to specific elements of the NASA security program requires that the program or project manager and CCS/CCPS justify the waiver request through:

a. Security risk analysis, (e.g., cost of implementation);

b. Effect of potential loss of capability to the Center;

c. Compromise of national security information;

d. Injury or loss of life; loss of one-of-a-kind capability; or

e. Inability of the CCS/CCPS to perform its missions and goals.

(1) Justification will also include an explanation of any compensatory security measures implemented in lieu of specific requirements.

(2) The waiver request shall be submitted to the Center Director.

1.3.2 The Center Director shall either recommend approval or return the waiver request to the CCS/CCPS for further study or closure. The Center Director forwards concurrence to the Mission Support Directorate Associate Administrator.

1.3.3 The Mission Support Directorate Associate Administrator shall forward waiver requests to the AA, OPS requesting concurrence and/or comments or a return of the proposals to the Center director for further study or closure.

1.3.4 The AA, OPS, shall return the waiver request to the Mission Support Directorate Associate Administrator with a recommendation for approval of the waiver, for further study or denial.

1.3.5 The Mission Support Directorate Associate Administrator shall return the waiver requests to the Center Director with concurrence and/or comments or return proposals for further study or closure.

1.4 Violations of Security Requirements

1.4.1 Anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving the NASA personnel security program is subject to disciplinary action up to and including termination of employment and/or possible prosecution under 18 U.S.C. § 799, that provides fines or imprisonment for not more than 1 year, or both.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS